First County Bank
It's where you belong.

CustomerFirst
CONTACT CENTER
Weekdays 203.462.4400
Touch Tone 203.462.4300

Small Business Guide to Corporate Account Takeover

What is Corporate Account Takeover?

Corporate account takeover is a type of fraud where thieves gain access to a business's finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable.

Cyber thieves target employees through phishing, phone calls, and even social networks. It is common for thieves to send emails posing as a bank, a delivery company, court, or the Better Business Bureau. Once the email is opened, malware is loaded on the computer which then records login credentials and passcodes and reports them back to the criminals.

How do I protect myself and my small business?

Consider these tips to ensure your business is well prepared:

- **Educate your employees.** You and your employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.
- **Protect your online environment.** It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically.
- **Partner with us to prevent unauthorized transactions.** Talk to us about programs that safeguard you from unauthorized transactions. Positive Pay and other services offer call backs, multi-factor authentication, multi-person approval processes and batch limits that help protect you from fraud.
- **Pay attention to suspicious activity and react quickly.** Look out for unexplained account or network activity, pop ups, and suspicious emails. If detected, immediately contact your financial institution, stop all online activity and remove any systems that may have been compromised. Keep records of what happened.
- **Understand your responsibilities and liabilities.** The account agreement with your bank will detail what commercially reasonable security measures are required in your business. It is critical that you understand and implement the security safeguards in the agreement. If you don't, you could be liable for losses resulting from a takeover. Talk to us if you have any questions about your responsibilities.

Industry and Law Enforcement Warning to Businesses on Business Email Compromises

Several warnings were released to raise awareness regarding an increase in phishing scams targeting businesses in an attempt to compromise their accounts. Known as Business Email Compromise, this scam is conducted by cybercriminals who compromise legitimate business email accounts to impersonate executives and conduct the unauthorized transfers of funds. (See First County Bank's *Business Email Compromise* Customer Security Awareness document for more information.)

If you have any questions call our CustomerFirst Contact Center at (203) 462-4400

(Monday - Friday from 8:30 a.m. to 4:30 p.m.)